Kentucky Governor's Office for Technology

Security Awareness Newsletter

Published by the GOT Division of Security Services

September 2003 **Volume 1, Issue 6**

Inside this issue:

Network Traffic Update: Securing the Commonwealth's Intranet

This article is not about rush hour conditions on Kentucky roadways but rather the new network traffic restrictions on the Commonwealth's information highway. In July 2003, GOT began blocking certain traffic from entering the secured stated agency network (Intranet) in efforts to provide a more secure computing environment.

In accordance with the Enterprise Network Security Architecture Policy (CIO-074) and the Firewall & VPN Administration Policy (CIO-076), servers/services needing public visibility must *not* originate from within the Intranet. Any server or services requiring access by external Internet users or other Kentucky Information Highway (KIH) users not residing within the Intranet must be realigned into one of three security zones: the e-Government DMZ (demilitarized zone), a 3rd party hosting site, or the Extranet (requires a business case exception). *Note: The DMZ acts as a neutral zone between the secured internal network (Intranet) and the external public network (Internet), preventing outside users from acquiring direct access to servers that contain an agency's data.*

The services currently prohibited from entering the State's Intranet are:

- HTTP (HyperText Transport Protocol—web browser protocol)
- NetBIOS (Windows file sharing and printing services)
- DNS (Domain Name System—name resolution program for Unix & Internet)
- WINS (Windows Internet Naming Service—Windows name resolution software)
- SMTP (Simple Mail Transfer Protocol—standard email protocol for the Internet)

Other services soon to be blocked include FTP (File Transfer Protocol) and Telnet (terminal emulation protocol).

These services are frequent modes of attack for hackers wanting to gain remote access to a network. Following viruses and worms, reconnaissance attacks using these services are the most prevalent threat to the KIH. By blocking this traffic from the state's Intranet, the internal network will be more secure for the State's agencies.

Agencies were notified in advance of the network changes. Those agencies not in compliance as of July were asked to complete a waiver stating the agency's intent to bring the service into compliance by September 1, 2003. GOT is temporarily allowing these services to continue for those agencies that have submitted a waiver and are actively working to relocate servers/services to either the e-Government DMZ or a third party provider.

For more information on the new enterprise network security architecture, refer to Agency Contact Memoranda #2203–0701 & 0802 available in GOTSource.

Did you know . . .

GOT's Division of Security Services has investigated over 8,500 IT security incidents since January of this year. The majority of incidents reported are related to unsolicited email (spam) and viruses & worms.

Upcoming SPPM Review

GOT is scheduled to begin the update of the Security Policies and Procedures Manual (SPPM) in late September.

The SPPM is comprised of various IT security policies and procedures GOT staff must follow in their day-to-day business operations. All GOT staff and contractors are required to read and comply with the SPPM. The policy manual is intended to address a broad range of security related topics and is organized into the following subject areas:

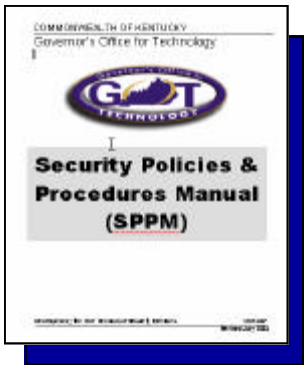
- Logical Security
- Managerial Security
- Physical Security
- Contingency Planning
- Security Awareness Program

The main purpose behind the SPPM is to educate and inform GOT staff of the security directives required to safeguard the Commonwealth's computing environment.

Representatives from various GOT organizations will once again be asked to participate in this year's revision, augmenting the SPPM to address GOT's evolving security requirements. In order to ensure the SPPM addresses all of GOT's security needs, it is important that various organizations have a voice in this task.

When the update is completed, GOT staff will be sent a notice outlining this year's changes, as well as a link to access the manual in GOTSource.

"All GOT Staff and contractors are required to read & comply with the SPPM"



A Worm by Any Other Name . . .

August was a banner month for computer viruses & worms invading the Kentucky Information Highway. Many agencies at both the state & local levels experienced network disruption from several worms including Lovsan/Blaster, Nachi, and Sobig.

With all of the recent malicious code activity, one might wonder how in the world do they come up with those names? Well according to an article in CNET, the folks at the Computer Antivirus Research Organization (CARO) are responsible for computing up with those strange names. The virus experts use what they call the CARO naming convention to assign descriptive names to all malicious code.

The first part of the worm/virus name usually designates if it is a Trojan horse, Visual Basic script, or a 32-bit Windows virus. This is followed by the virus family or group name, and whether or not it is an email or mass mailing virus. The official name of Sobig, which is W32.Sobig.F@mm, can be dissected to divulge the following information:

- **W32** indicates that it is a 32-bit Windows worm, which means it affects only 32-bit Windows platforms.

- **Sobig** identifies the worm's family name.

- **F** indicates the variant of the worm. Yes, that means that Sobig.F probably had several predecessors such as Sobig.A, Sobig.B, and so on.

- **@mm** signifies that the worm is a mass mailing worm. In other words, it can send itself to every address in your Outlook address book.

Sounds like the virus industry has its act together, doesn't it? Well, not exactly. Many anti-virus companies such as Symantec, NAI (McAfee), and Sophos tack on their own prefixes & suffixes to malicious code names. This was especially true for the Lovsan/Blaster worm, which went by 11 different aliases. Talk about confusing. The good thing is that as long as you keep your virus definition files (DAT) updated, your anti-virus protection software won't care that

"Many antivirus companies… tack on their own prefixes & suffixes to malicious code names"

Blaster also goes by MSBlast, MSBlast.A, Lovsan, W32/Lovsan… well you get the picture.

To learn more about virus monikers, check out this Symantec webpage.

Attack of the Network Worms or How My PC Took on a Life of Its Own

August 2003 started out normal enough. Just a month like any other. The worst to be expected was maybe a minor virus outbreak here or there on the KIH. Nothing to rile usual network operations. But it just wasn't meant to be . . .

On August 1st, we saw an ominous outbreak of the Mimail worm. Fortunately, infection of KIH devices was kept to a minimum by GOT filtering incoming infected attachments on the Internet mail scanner. But the horror didn't end there.

On August 15, the widely publicized Lovsan/Blaster worm hit the KIH. (Lovsan/Blaster exploits a Microsoft Windows operating system vulnerability.) The impact of Lovsan/Blaster caused minimal network disruption; however, it was the impact of a so called "good Samaritan" worm, Nachi, which was created to counteract Lovsan/Blaster, that caused network administrators and users alike to shake their heads in horror. The Nachi worm quickly spread over the KIH, infecting devices on both the internal and external networks. The number of devices infected is estimated to be in the thousands.

Due to Nachi's payload, which included the download of the MS patch to prevent Lovsan/Blaster infection, a denial of service type effect was experienced on the network, impacting email and Internet services and generally decreasing network performance.

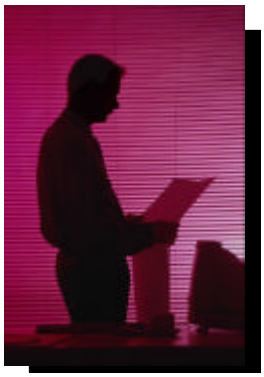
But wait… there's more. Another outbreak occurred the same time as the Lovsan/Blaster and Nachi worms. The Sobig.F worm, which was reported to have a time bomb-like payload that was scheduled to activate on August 22 to gather the addresses of computers previously

compromised, and launch an unknown, pre-programmed attack. Fortunately, Sobig was more bark than bite and the impact on the KIH was not as severe as previous worms.

To prevent and lessen the next outbreak, GOT recommends agencies always install the latest hardware and software patches to correct any vulnerability. Lovsan/Blaster took advantage of one such security hole that could have been prevented if the appropriate Microsoft patch had been installed. Also, always keep your anti-virus protection software's virus definition files (DAT) updated. This will help protect your PC from the latest threats and will also help you sleep better at night knowing the nightmare was just a bad dream . . .

To help agencies and GOT staff keep abreast of the latest malicious code threats and hardware/ software security vulnerabilities, GOT has a webpage that has all the latest security info.

Safeguarding Sensitive Documents: Watch out for Prying Eyes!



There may be times when you need to print sensitive or confidential business documents that you would rather other people did not see. Or maybe you need to dispose of a report that contains social security numbers and/or other personal identifying information. Be aware of prying eyes that are on the look out for such information.

Those eyes may belong to someone who is simply curious or nosey or, even worse, they may belong to a social engineer who is looking for social security numbers or other personal information to steal a person's identity.

Here are a few common sense tips to help you safeguard confidential data:
- *Immediately pick up sensitive documents from the printer after printing.*
- *Never throw sensitive documents in the garbage can or recycle bin. Instead use a shredder. Most GOT printers have a shredder located nearby just for this purpose.*
-*Always remember to remove original documents from the copy machine after copying.*

By following these simple tips, you can ensure that your documents are "for your eyes only."

Intro to PKI: What It is and How It is Used

Everyday the Internet continues to transform the way we do business. Many business transactions can now be performed online, whether it be ordering office supplies, filing taxes, or even renewing one's car tags.

Due to dwindling fiscal resources, government entities are also looking to the Internet to provide services to its citizens, reducing administration costs and increasing convenience by bringing government to the people.

That is where PKI comes into the picture. PKI or Public Key Infrastructure is an encryption system based on keys. PKI enables users to utilize the Internet to privately and securely exchange money and/or data through the use of public & private keys and encryption. These keys ensure a certain level of trust for users and also can serve as a means to verify a person's identity when conducting business over the Internet.

In a paper-based world, we use our handwritten signature and/or a form of identification such as a driver's license to prove our identity. In the digital world, we will use a digital ID as a means of authentication. A digital ID is basically

"In a paper based world, we use our signature to prove our identity . . . In the digital world, we will use a digital signature as a means of authentication"

an electronic signature that is used to authenticate the identity of the sender of a message or the signer of a document. In other words, it acts as a notary public to validate your signature—to verify you are who you say you are. You can then use your digital ID to sign email, documents, and even web forms. You can also use your digital ID to encrypt data in email, sensitive documents, and on web pages.

If you have ever used encryption software such as PGP (Pretty Good Privacy), then you probably have a fairly good understanding how PKI works. There are two keys, both a public and private key that are created when a user first generates their profile. The public key can be accessed through email or a common directory to those who need to communicate with the user. Messages and data are encrypted using the public key and then sent to the user, who decrypts the message with their private key.

A corporate PKI system is based on the same principle but it much more complex in that it has a high administration overhead in issuing keys, revoking keys, security management, authentication controls, etc.

The Commonwealth is currently operating as a Certificate Authority (CA), which means it is issuing digital certificates used to create digital signatures and public-private key pairs. Kentucky state government has selected the Entrust suite of PKI enabled products for digital signature technology and securing email transport of contents & attachments. For more information on the enterprise standard, click here.

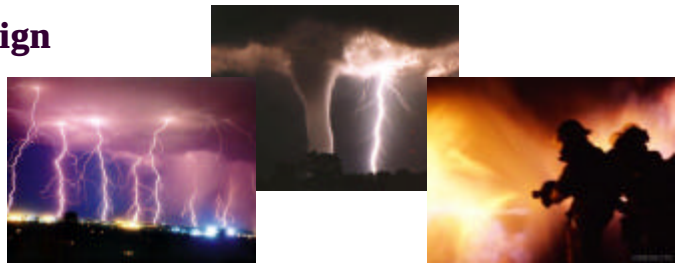
How to Spot an Email Hoax

So you just received an email from Bill Gates offering you free British Airways tickets. Or maybe you received that email that warns you to watch out for the new mobile phone virus that will infect your phone if you answer calls that displays "unavailable" on the screen.

These are just a couple of examples of hoax emails that are circulating the Internet these days. But how do you know what to believe and what not? There are several websites that specialize in email hoaxes. If you're unsure of the validity of a particular email, check out CIAC's HoaxBuster website, McAfee's Virus Hoaxes web page or Symantec's Hoax web page. If it is a hoax, it will probably be listed on one of these websites. Many hoaxes urge readers to "send this to everyone you know." That should be a red flag that it is a hoax or virus or both. Forwarding these emails only clogs up the network and could aid in propagating viruses.

Always keep the following motto in mind: ***If in doubt, don't send it out!***

Disaster Recovery Awareness Campaign

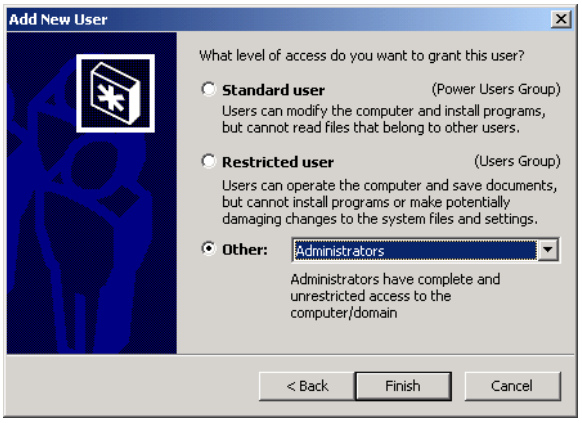


The Governor's Office for Technology is gearing up for its new awareness campaign for disaster recovery and planning. Disaster recovery planning is a crucial process in restoring vital systems after a disaster or other catastrophic event.

GOT's primary goal for this campaign is to educate and inform staff and customers of the importance of disaster recovery planning in protecting the Commonwealth's computing environment. Starting in November, GOT will include articles in this newsletter which highlight the latest issues in disaster recovery planning, awareness, and prevention measures, including information on industry best practices and frequently asked questions to provide readers with a comprehensive grasp of their role in the disaster recovery process. We will also be creating a GOT-Source library of informative articles which should help to inform and educate.

GOT is also interested in anyone with artistic talent to help design a cartoon logo with an appropriate disaster recovery related theme to be used on posters, mouse pads, etc. If you are interested, contact Tom Van Horn via email or at 502.564.5769.

The Scoop on Admin Accounts



An administrator account is generally an account assigned to the network administrator(s) responsible for setting up users accounts, granting file permissions and performing general administration of the network. *(To prevent accidental user mishaps, it is best practice to assign the admin account to a function (network administration) not a person.)*

Admin accounts have the highest permission levels of all accounts, making them favorite targets of hackers and network intruders. For this reason, it is a good idea to rename the administrator account to something less obvious making it more difficult for hackers to discover. By renaming the account, it makes it harder for the hacker to guess the account name, as well as the password, discouraging them from using automated tools to crack the password since they do not know which account id is the admin account. While this is not totally fail proof since hackers have tools that can determine account type based on certain criteria, why make it any easier for an intruder to gain access to network. In accordance with GOT Policy, it is also a good idea to use the Passprop utility to enable admin account lockout after three unsuccessful password attempts. This will lock the local administrator account remotely but will still allow login locally. Please note this procedure is not recommended for domain controllers. Network administrators should also use the appropriate O/S version of the Passprop utility found in the network operating system's resource kit.

Now that you've renamed the admin account, be sure that the admin password is a complex, policy-compliant password. Admin passwords should be at least **11 characters in length** and should be composed of following criteria:

- **Upper and lower case letters**
- **Numbers**
- **At least one special character.**

For more information on creating strong passwords, click here.

Cyber Bytes

Creators of Lovsan/Blaster Variants Arrested

Two men who are believed to be the writers of two variants of the Lovsan/Blaster worm that infected PCs worldwide in late August have been arrested.

Jeffrey Parson, 18, is accused of writing Lovsan.B and Dan Dumitru Ciobanu, 24, a Romania University student, is purported to be the creator of Lovsan.F.

The creator of the original worm, Lovsan.A, has not yet been caught. It is estimated that the worm cost companies $1.3 billion in damages and lost productivity.

— Condensed from Information Security Magazine

". . . the worm cost companies $1.3 billion in damages & lost productivity"

Security Experts Testify Before Congress

Security experts and industry executives testified before Congress on September 9 to bolster the nation's preparedness against cyber threats such as viruses & worms.

The congressional meeting focused on providing viable solutions to the ever-increasing incidence of spam and malicious code.

The group also discussed ways to encourage software vendors to prioritize making their software more attack resistant.

—Condensed from Eweek

Microsoft Opens Office Online

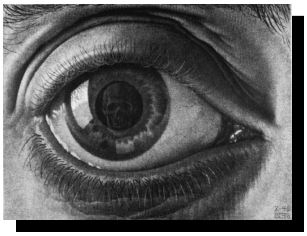
Microsoft recently launched Office Online, an updated version of its resource tools website giving users access to templates, clip art, and other information designed to help them use Office more effectively. The site's address is Office.Microsoft.Com.

RIAA Hit List—Are You on their List?

The Recording Industry Association of America has issued more than 900 subpoenas for users illegally swapping music files. According to TechTV.com, the RIAA is still gunning for people offering songs on file-sharing networks such as KaZaA and Grokster. If you want to find out if your username is on the list, visit the RIAA website.

—Condensed from TechTV.com

Big Brother is Watching You!



You can already be tracked through your cell phone, but new technology is being introduced that can be installed in household items, tipping off police if they are stolen. Televisions, DVDs, & computers may eventually be fitted with a chip that transmits their location. There is even talk in Britain about installing chips in cars to automatically prevent them from exceeding the speed limit. You can read more on this subject at Wired.com.

Microsoft Information

IE Patch Does Not Work

According to industry security expert, eEye Digital Security, a patch released by Microsoft to fix a critical security flaw in Internet Explorer does not work. The vulnerability was discovered by eEye Digital Security four months ago. Microsoft released a patch on August 20 and then re-released it on August 28 because there were problems with some non-default operating system installations. According to eEye, the patch appears to be due for yet another re-release because it does not fix the vulnerability it is supposed to. This IE flaw can be exploited by someone coding a HTML file that extracts and executes malicious code when it is viewed in the IE browser.

A Microsoft representative said it was investigating the eEye report but had not received reports from any customers being affected by the claimed variation of the original vulnerability. Microsoft will continue to distribute the original patch and recommends users who haven't applied it, do so promptly.

Concerned users can disable active scripting on their browsers to mitigate the vulnerability until Microsoft updates the patch. For more information, click here.

Information for this article was gathered from the C/Net article, "Security Firm: IE Patch Does Not Work" by Patrick Gray.

Microsoft Windows Vulnerability—MS03-034

A security issue affecting Windows NT 4.0 Server, Windows Server 2003, Windows 2000 and Windows XP could allow an attacker to see information in your computer's memory over a network. Microsoft recommends that you apply their patch as soon as possible. Click here for more information and instructions for downloading the patch.

MS Word Flaw—MS03-035

A flaw has been identified in MS Word that could allow an attacker to compromise a Windows-based system possibly allowing a hacker to read files on your computer or run programs on it. Microsoft has released a patch for this vulnerability. Click here for more information.

Security Update for Office—MS03-036

A vulnerability affecting MS Office 97, 2000, & XP could allow a hacker to read files on your system or run programs on it. This vulnerability also affects Word 98, FrontPage 2000 & 2002, Publisher 2000 & 2002, and Work Suites 2001, 2002, & 2003. Click here for more information.

Security Update for VB for Applications—MS03-037

A flaw in MS Visual Basic for Applications may allow a hacker to comprise your system. Microsoft rates this update as critical so you should patch your systems as soon as possible. For more information, click here.

MS Windows RPCSS Service Flaw—MS03-039

Critical flaws involving the Microsoft Windows RPCSS service have been recently discovered. A remote attacker could exploit these vulnerabilities allowing them to run malicious code on vulnerable systems and possibly launch denial of service (DoS) attacks. This applies to server and client versions of Windows NT, 2000, 2003, as well as windows XP. For more information, click here.

KENTUCKY GOVERNOR'S OFFICE FOR TECHNOLOGY

Division of Security Services
101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502-564-7680
Email: GOTSecurityServices @mail.state.ky.us

We're on the Web!
ky.gov/got/security/

GOT's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security and information systems professionals with timely information on cyber vulnerabilities, information security trends, virus information, and security policies and practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of the GOT Security Policies and Procedures Manual (SPPM), GOT's disaster recovery/ business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, and Unix Solaris & AIX systems. DSS also provides mainframe RACF, computer forensics, and password auditing services to state agencies upon request. If you would like to learn more about the services that DSS provides, visit our web page at ky.gov/got/ security.

For more information on IT Security, check out the following websites!

www.cert.org—The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com—Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com—Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence Service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through email, voice message, fax, or SMS (Small Message Service) on wireless phones.

www.zdnet.com—ZDNet operates a worldwide network of websites for people who want to buy, use, and learn about technology.